State of Illinois
Department of Innovation & Technology

Enterprise Information Security Policy

Configuration Management

1. OVERVIEW

The State of Illinois Department of Innovation & Technology (DoIT) is responsible for the establishment and implementation of appropriate configuration management controls that safeguard the confidentiality, integrity, and availability of Information Systems. This Policy alleviates security risks through configuration management processes. Unless otherwise specified, capitalized terms contained herein shall have the meaning assigned to them in the Terminology Glossary.

2. GOAL

The goal of this Policy is to create a prescriptive set of process and procedures, aligned with applicable DoIT information technology (IT) security policies and standards, to ensure that DoIT develops, disseminates, and updates its configuration management practices. This Policy establishes the minimum requirements for configuration management.

Executive agencies, boards, and commissions are required to implement necessary controls to maintain proper documentation of IT Resources and information assets on the basis of business and security requirements.

3. SCOPE

This Policy applies to Employees of DoIT and other State of Illinois agencies, boards, and commissions that have been identified as client agencies of DoIT through executive order, legislation, or inter-governmental agreement (Client Agencies).

4. REQUIREMENTS

DoIT and/or its Client Agencies will incorporate the below defined information security controls for all Information Systems. Any reference to "Agency" below shall include both DoIT and Client Agencies.

4.1 Baseline Configuration

4.1.1 DoIT shall develop, document, and maintain under configuration control a current baseline configuration of the Information System that:

- maintains baseline configurations of the Information System to be consistent with State of Illinois Agencies' enterprise architecture;
- maintains records that document the application of baseline security configurations;
- monitors systems for security baselines and policy compliance;
- reapplies all security configurations to IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade; and
- modifies individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.

4.1.2 Agency shall create and periodically review a list of Agency hardware and software assets.

4.1.3 DoIT shall review and update the baseline configuration of the Information System:

- based on a defined frequency;
- when required due to a significant configuration change, such as an operating system upgrade or hardware change, or due to a demonstrated vulnerability; and

- as an integral part of Information System component installations and upgrades.

4.2 Configuration Change Control

4.2.1 DoIT shall determine the types of changes to the Information System that are configuration-controlled.

4.2.2 DoIT shall review and approve configuration-controlled changes to the system with explicit consideration for security impact analyses.

4.2.3 DoIT shall document approved configuration-controlled changes to the system.

4.2.4 DoIT shall retain and review records of configuration-controlled changes to the system.

4.2.5 DoIT shall audit and review activities associated with configuration-controlled changes to the Information System.

4.2.6 DoIT shall coordinate and provide oversight for configuration change control activities through a committee that convenes based on an approved frequency to review changes prior to implementation.

4.3 Security Impact Analysis

4.3.1 Agency shall analyze changes to the Information System to determine potential security impacts prior to change implementation.

4.4 Access Restrictions for Configuration Changes

4.4.1 Agency shall define, document, approve, and enforce physical and logical access restrictions associated with changes to the Information System.

4.4.1.1 Only qualified and authorized individuals are allowed to obtain access to Information System components for purposes of initiating changes, including upgrades and modifications.

4.4.1.2 Maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the Agency become aware of an unauthorized change to the Information System.

4.4.1.3 Logical and physical access control lists that authorize qualified individuals to make changes to an Information System or component must be created and maintained by the Agency.

4.4.1.4 Access to software libraries is restricted to authorized individuals.

4.4.2 Agency shall limit Information System developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment.

4.4.3 Agency shall review and update Information System developer/integrator privileges annually.

4.5 Configuration Settings

4.5.1 DoIT shall establish, document, and implement the configuration settings for IT services.

4.5.2 DoIT shall identify, document, and approve exceptions from the established configuration settings for individual components within the Information System based on operational requirements.

4.5.3 DoIT shall monitor and control changes to the configuration settings in accordance with relevant policies and procedures.

4.6 Least Functionality

4.6.1 DoIT shall verify that the Information System is configured to provide only essential capabilities.

4.7 Information System Component Inventory

4.7.1 DoIT shall develop, document, and maintain an inventory of Information System components that:

- accurately reflects the current Information System;
- includes components within the authorization boundary of the Information System;
- is at the level of granularity deemed necessary for tracking and reporting; and
- includes Agency-defined information deemed necessary to achieve effective property accountability.

4.7.2 DoIT shall review and update the Information System component inventory annually.

4.8 Configuration Management Plan

4.8.1 DoIT shall develop, document, and implement a configuration management plan for the Information System.

5. POLICY COMPLIANCE

In order to implement this Policy, the DoIT Division of Information Security may establish supplemental policies, standards, procedures, and guidelines and may designate responsibility to specific personnel. To the extent necessary, each Client Agency and/or DoIT Division must establish procedures in order to achieve Policy compliance. It is the responsibility of Employees to understand and adhere to this Policy.

Failure to comply with this Policy may result in the Chief Information Security Officer temporarily discontinuing or suspending the operation of the Information System, solution, and/or resource until such compliance is established as deemed solely by the Chief Information Security Officer. Failure to comply with this Policy could also result in the loss of access to State of Illinois IT Resources and/or discipline, up to and including discharge.

6. RELATED POLICIES, STANDARDS, AND GUIDELINES

DoIT Supplemental Information Security Policies:

(1) Criminal Justice Information Security
(2) Federal Tax Information Security
(3) Payment Card Data Protection
(4) Protected Health Information Security

Revision history and approvals are reflected in ServiceNow.